

## 29 . プロシージャ配布の標準

0.91 版

### ----- 取扱注意事項 -----

特定非営利活動法人日本ネットワーク・セキュリティ協会（JNSA）のセキュリティポリシーワーキンググループにて作成した「情報セキュリティポリシーサンプル」（以下、ポリシーサンプル）をご参照、ご利用される場合、以下の事項に従ってください。

#### 1. 公開の目的

- 1-1. セキュリティポリシーを作成する際の参考
- 1-2. 既存のセキュリティポリシーとの比較によるレベル向上
- 1-3. 既存のセキュリティレベルの大きな把握

#### 2. ご利用にあたっての注意事項

- 2-1. ポリシーサンプルの著作権は、NPO 日本ネットワークセキュリティ協会（JNSA）に属します。
- 2-2. ポリシーサンプルへのリンクは、JNSA 事務局（sec@jnsa.org）への一報をもってフリーです。  
ただしリンクには必ず JNSA サイトのトップページ(<http://www.jnsa.org/>)を指定してください
- 2-3. ポリシーサンプルの全文もしくは一部を引用する場合には、必ず引用元として「JNSA セキュリティポリシーWG 作成ポリシーサンプル」を明記して下さい。営利目的、非営利目的の区別はありません。

ポリシーサンプルの全部あるいは一部をそのまま、ご使用いただく場合：

【出典】「情報セキュリティポリシーサンプル(0.91 版)」

NPO 日本ネットワークセキュリティ協会(JNSA) <http://www.jnsa.org/>

ポリシーサンプルを一部加工して、ご使用いただく場合：

【参考文献】「情報セキュリティポリシーサンプル(0.91 版)」

NPO 日本ネットワークセキュリティ協会(JNSA) <http://www.jnsa.org/>

- 2-4. ポリシーサンプルを利用したことによって生ずるいかなる損害に関しても JNSA は一切責任を負わないものとします。
- 2-5. 本ポリシーサンプルを報道、記事など、メディアで用いられる場合には、JNSA 事務局にご一報ください。

#### 3. ご意見等連絡先

ポリシーサンプルに関するご意見・ご感想・ご質問等がありましたら、JNSA 事務局まで E-Mail にてご連絡ください。ただし勧誘、商品広告、宗教関連、チェーンメールの E-Mail はお断りします。

また、E-Mail にファイルを添付する場合は、添付するファイルをアンチウイルスソフトウェア等で予め検査を行ってください。

URL : <http://www.jnsa.org> E-Mail : [sec@jnsa.org](mailto:sec@jnsa.org)

## 29 . プロシージャ配布の標準

### 29 . 1 趣旨

本標準は、規定された、または更新されたプロシージャを、対象者に適切に配布し周知することを目的とする。

### 29 . 2 対象者

プロシージャの開示を許可されたすべての従業員

### 29 . 3 対象システム

本標準はプロシージャ配布に関するものであり、情報システムや情報機器を対象としない。

### 29 . 4 遵守事項

#### 29 . 4 . 1 対象者への周知

- ( 1 ) 情報セキュリティ委員会は、プロシージャの制定、および更新を実施した場合、迅速に開示が許可された対象者へ周知しなければならない。

#### 29 . 4 . 2 配布の手段

- ( 1 ) 情報セキュリティ委員会は、プロシージャを Web 上で公開する。
- ( 2 ) Web サーバへのアクセスは、開示が許可された対象者のみが閲覧できるように正しく制御されなければならない。
- ( 3 ) 情報セキュリティ委員会は、ネットワーク上の問題等によってプロシージャの閲覧ができなくなることを避けるために、一定数の紙媒体によるプロシージャを保有していなければならない。

#### 29 . 4 . 3 対象者の確認

- ( 1 ) 情報セキュリティ委員会は、Web ベースによる理解度チェック問題など、

対象者の理解度を確認するための手段を用意しなければならない。

- (2) 対象者は、情報セキュリティ委員会からの周知を受けてから、速やかにプロセスの内容を確認し、理解しなければならない。
- (3) 対象者は、情報セキュリティ委員会が用意した理解度確認用の手段を、周知後1週間以内に実施しなければならない。

#### 29.4.4 実施の確認

- (1) 情報セキュリティ委員会は、対象者が理解度確認の手段をすべて実施し、必要な条件を満たすことにより、プロセスを受け取り正しく理解したとみなすことができる。
- (2) 各部署のセキュリティ責任担当者は、各担当者の実施状況を Web のツールで確認することができる。セキュリティ責任担当者は、未実施者を識別し、未実施者に対して実施を促さなければならない。セキュリティ責任担当者は、やむを得ない理由で対象者の実施が困難な場合、速やかに情報セキュリティ委員会に報告しなければならない。

#### 29.5 例外事項

業務都合等により本標準の遵守事項を守れない状況が発生した場合は、情報セキュリティ委員会に報告し、例外の適用承認を受けなければならない。

#### 29.6 罰則事項

本標準の遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合がある。罰則の適用については『罰則に関する標準』に従う。

#### 29.7 公開事項

本標準は対象者にのみ公開するものとする。

#### 29.8 改訂

・本標準は、平成××年××月××日に情報セキュリティ委員会によって承認され、平成××年××月××日より施行する。

・本標準の変更を求める者は、情報セキュリティ委員会に申請しなければならない。情報セキュリティ委員会は申請内容を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

・本標準は、定期的（年1回）に内容の適切性を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

#### 用語集

（特になし）